DEFENSE INTELLIGENCE AGENCY STAFF SUMMARY SHEET

ORIGINATOR (Symbol)	TELEPHONE NO	DATE
RSE-4		26 April 84
AC		

SUBJECT
DoD Trusted Computer System Evaluation Criteria

REMARKS
1. PURPOSE: To provide the DIA position on the DoD Trusted Computer System Evaluation Criteria as a proposed DoD Standard to the Deputy Under Secretary of Defense for Policy (DUSD(P)).

2. BACKGROUND: The criteria defined in the document were developed by NSA and other DoD components and constitute a uniform set of basic requirements and evaluation classes for assessing the effectiveness of security controls built into computer systems. These criteria are intended for use in the evaluation and selection of computer systems being considered for the processing of sensitive or classified information by the DoD. Last August, NSA published the criteria without formal coordination. DUSD(P) has now required NSA to coordinate the document.

3. DISCUSSION: The criteria requires the protection of System High systems at a level designed for Compartmented Mode systems. This is neither reasonable nor economically feasible. The document also allows a user operating at one security level to create data to be stored at a higher security level, which poses a denial of service and disinformation threat. Incorporation of the modifications recommended by DIA would make the document acceptable. DIA has previously attempted to have the document changed but our proposed changes were consistently ignored by NSA. DIA considers the criteria to be evolving guidelines and will apply them individually and selectively as necessary to meet operational and system design requirements. It may be necessary to exempt systems already under development and current operational systems from the criteria because of the high costs incurred in retrofitting security. A background paper and copy of the criteria are attached. The Director has also requested that a personal letter be provided to Director, NSA with copy of DUSD(P) memo and DIA position attached.

4. CONCLUSION: DIA should non-concur in the criteria until modifications requested in the enclosure to facing memorandum are incorporated into the document.

5. RECOMMENDATION: DR signature on facing memorandum to DUSD(P) and personal letter to DIRNSA.

STAT

2 Enclosures
1. Background Paper, 1 cy
2. DoD Trusted Computer Systems Evaluation Criteria, 1 cy

Deputy Director for Resources and Systems

DIA FORM 1 OCTOBER 1962 (Previous edition will be used until exhausted) DIAR 12-8

GPO : 1983 O - 407-029

ENCLOSURE TO STAFF SUMMARY SHEET

BACKGROUND:

The DoD Trusted Computer System Evaluation Criteria document was developed by the DoD Computer Security Evaluation Center (CSC) which is attached to NSA. We will hereafter refer to this document as the CSC CRITERIA.

The Criteria defined in the CSC CRITERIA constitute a uniform set of basic requirements and evaluation classes for assessing the effectiveness of security controls built into computer systems. These criteria are intended for use in the evaluation and selection of computer systems being considered for the processing of sensitive or classified information by the DoD. The Criteria classify systems into four broad hierarchial divisions of enhanced security protection and they provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products. The Criteria were developed with three objectives in mind: (a) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; (b) to provide guidance to manufacturers as to what to build into their new trusted commercial products; and (c) to provide a basis for specifying security requirements in acquisition specifications. Two types of requirements are delineated for secure processing: (a) specific security feature requirements and (b) assurance requirements. Some of the latter requirements enable evaluation personnel to determine if the required features are present and functioning as intended. Though the criteria are application-independent, it is recognized that the specific security feature requirements may have to be interpreted when applying the criteria to specific applications or other special processing environments. The underlying assurance requirements can be applied across the entire spectrum of ADP system or application processing environments without special interpretation.

The CSC CRITERIA is proposed as the DoD Standard but is does not meet the needs of the Sensitive Compartmented Information (SCI) community within DoD. The new document's protection functionalities do not coincide with the existing SCI requirements of System High and Compartmented modes. If the existing SCI requirements were required to be adjusted to match the new proposed standard's levels, both the System High and Compartmented Mode requirements would have to be individually adjusted up or down on the new proposed scale to either more or less stringent security protection levels. Neither of which is acceptable to the SCI community. The adjustment to conform with this document's security requirements would cause either a weakening of current security for System High accredited systems or an unreasonable expenditure of funds in order to strengthen these systems to meet the document's security criteria at the next highest level.

The CSC CRITERIA was developed under DoD Directive 5200.28. DoDD 5200.28 generally provides the security policy for collateral systems. SCI, SIOP-ESI, RESTRICTED DATA or FORMERLY RESTRICTED DATA, and Critical Nuclear Weapons Design Information all must meet minimums provided in documents other than DoD Directive 5200.28. The CSC CRITERIA does not reference these other minimums.

For Sensitive Compartmented Information (SCI) the Director of Central Intelligence is the statutory authority. His authority originates in the National Security Act of 1947 and several Executive Orders.

The Director, DIA is the Senior DoD Intelligence Officer. As such, he is a National Foreign Intelligence Board (NFIB) member and the Executive Agent for the Secretary of Defense, Joint Chiefs of Staff, and the Military Services for all matters concerning intelligence, except for those matters reserved for the Director NSA. Those being Communications Security (COMSEC, including CRYPTOGRAPHIC and CRYPTOLOGIC subsets); CRYPTOANALYTIC; and Signal Intelligence (SIGINT) collection, processing, and dissemination.

Clearly then, the appropriate authority for SCI within the DoD is the Director, DIA with DIA Manual 50-4, "Security of Compartmented Computer Operations" being the definitive document in terms of protection of SCI ADP systems subject the authority of the Director, DIA. The CSC CRITERIA is not oriented to the SCI community and does not even reference an SCI policy document in its list of reference.

Over the course of the CSC Criteria development, DIA has expressed its concerns to CSC through both formal and informal channels. When the current version (15 AUG 83) of the CSC Criteria was issued unilaterally by CSC as a DoD Standard, DIA's expressed concerns had produced little change in the CSC Criteria.

Eventually the lack of formal coordination prior to promulgating a DoD Standard was noticed and DUSD(P) disseminated copies of the CSC CRITERIA in accordance with the formal DoD coordination process. This reply to DUSD(P) is in response to the formal coordination request.

DUSD(P) has disseminated copies of the CSC CRITERIA for formal coordination within DoD.

DISCUSSION:

The CSC CRITERIA establishes a series of protection levels and sublevels for the certification of computer systems. The levels of divisions in increasing levels of protection and their DIAM 50-4 counterparts are:

CRITERIA DIVISION	CRITERIA PROTECTION	DIAM 50-4
"D"	MINIMAL	Dedicated Mode
"C"	DISCRETIONARY	Systems High Mode
"B"	MANDATORY	Compartmented Mode
"A"	VERIFIED	

SCI systems accredited for the Systems High Mode of operation under DCID 1/16 and DIAM 50-4 are systems accredited to provide need-to-know protection but not to guarantee the separation between data in different SCI compartments or subcompartments. The separation of need-to-know is the definition of DISCRETIONARY PROTECTION while the separation for compartments or security levels is MANDATORY PROTECTION.

The protection levels offered by the CSC CRITERIA under DISCRETIONARY PROTECTION are insufficient for the level of protection required for System High accreditation for foreign intelligence systems under DCID 1/16 and DIAM

50-4. Changes to the DISCRETIONARY PROTECTION DIVISION are needed to strengthen the security protection offered in order for the CSC CRITERIA to match the DIAM 50-4 accreditation requirement for System High systems.

Under the CSC CRITERIA as currently written, in order to gain the protection necessary for SCI System High accredited systems, the certification level would have to be raised to the MANDATORY PROTECTION level. Which, by definition, is the protection designed for Compartmented Mode systems. Protecting DoD SCI System High systems to the same level as Compartmented Mode systems, which have not yet been operationally reached in DoD, is neither reasonable nor economically feasible. Additionally it is not even necessary if the CSC CRITERIA are adjusted. A small increase in the levels of protection offered in the DISCRETIONARY PROTECTION DIVISION of the CSC CRITERIA would satisfy the DCID 1/16 and DIAM 50-4 requirements for System High system protection, rather than the larger step up into the MANDATORY PROTECTION DIVISION.

This small increase in the protection offered in the DISCRETIONARY PROTECTION DIVISION is the essence of the DIA position and what DIA proposes in the attached DIA comments to the CSC CRITERIA document.

DIRECTOR
DEFENSE INTELLIGENCE AGENCY

Lieutenant General Lincoln Faurer, USAF
Director, National Security Agency
Fort George G. Meade, Maryland 20755

Dear Linc:

As you know, OSD has formally coordinated your proposed DoD Trusted Computer System Evaluation Criteria and requested my review and comments. As outlined in the attached memorandum to General Stilwell (enclosure 1), I am very appreciative of the initial efforts of your staff and the Computer Security Evaluation Center (CSEC) efforts to develop an initial set of criteria. It has been a large undertaking and certainly an important initiative for guiding users and manufacturers.

As indicated in the memorandum, it appears some significant shortfalls exist with respect to treatment of Sensitive Compartmented Information (SCI) handling in the evaluation criteria. An established system of periodic review is also needed to insure that the criteria do not become dated. These concerns and others have been detailed to General Stilwell and a copy is attached as enclosure 2.

I know the importance that you place on computer security and I share your concern for the critical importance of improving security, particularly in light of the

increased dependence on computers and communications in the Intelligence Community. However, given the potential cost implications, I believe the computer security standards and evaluation criteria must be comprehensive, fully coordinated, and be considered as guidelines which we can tailor to accommodate operational requirements.

I encourage a direct dialogue between our staffs to present these views. My staff is also available to assist in inserting our revisions into the document.

Sincerely,

2 Enclosures a/s

JAMES A. WILLIAMS
Lieutenant General, U.S. Army